



SNOW RISK MONITOR

Protect data and reduce risk

Reveal the hidden data risks lurking in your IT estate.

Today's IT environments are continually expanding, networked and running a myriad of different applications. As the digital landscape changes rapidly, how are IT leaders to secure their businesses from malicious attacks? The saying goes, "You Can't Protect What You Can't See" – and yet businesses face mounting challenges in gathering a holistic view of the IT estate, let alone the risks within.

To succeed, businesses must begin from a place of complete visibility into their assets and software.

In addition, they need to ensure that any personal data held on their systems is managed and controlled in accordance with the appropriate data protection regulations, like GDPR. IT leaders need to easily identify where vulnerabilities reside, or personal data is held, to mitigate risks associated with breach of privacy laws. With context around those vulnerabilities, you can decide exactly what to remediate first and go straight to the problem.

ASSET VISIBILITY – THE STARTING POINT TO REGULATORY COMPLIANCE

Snow Risk Monitor provides complete visibility of all devices, users and applications across on-premises, cloud and mobile. Automated discovery provides a detailed account of which users have access to which applications and cloud services, and how they are used. Utilizing the unique contextual capabilities inherent within the Snow platform, applications are also classified to highlight where personal data could be stored and processed, and the type of data held.

SOFTWARE VULNERABILITIES – THE THREAT HIDING IN YOUR SYSTEMS

Analysts predict by the year 2022, the increasing remote workforce and explosion in 3rd-party tools means that 50% of IT initiatives will be driven by security needs.*

How is your organization leveraging your ITAM inventory as a basis for security today?

Snow Risk Monitor helps mitigate cyber security risks by checking all applications against the best vulnerability information available - NIST's (National Institute of Standards and Technology) National Vulnerability Database – and flagging those with known vulnerabilities.

*Gartner (2019): IT Asset Management Must Rapidly Evolve to Address Emerging Business Risks

Benefits

IDENTIFY VULNERABILITIES ACROSS YOUR ENTIRE ESTATE

- Find all known vulnerabilities – not just the ones in the big data processing applications
- See which vulnerable applications are in use and where they reside on your estate
- Identify attack vectors of the path of a vulnerability

CATEGORIZE RISK TO PRIORITIZE

- Review upcoming End-of-Life and End-of-Support dates to minimize risk and maintain compliance
- Prioritize remediation effort based on NVD severity level
- Identify possible data leaks

MONITOR AND PROTECT PERSONAL DATA

- Identify applications processing personal data
- See the type of personal data applications being processed by applications
- Know which applications are installed on each device and who has access to them

PROTECT REPUTATION AND BUDGETS

- See severity level of identified risks based on augmented data sets
- Understand organizational risk with an overall scored risk metric
- Identify the spread of data across the business

UNPARALLELED, NEAR-TIME VISIBILITY

At Snow, we have 20 years of experience giving companies visibility into their digital technology landscape and have developed the most comprehensive, industry-leading library of software assets and versions (600k+ apps). These include End-of-Life and End-of-Support dates, normalized to display in language that's easily understood. Snow is uniquely positioned to take this intelligence (local, cloud and mobile), and cross-reference it to other data sources to provide insights. And with daily updates, you can be confident you're closing the gaps on risk, even as new vulnerabilities emerge

DATA-BASED RISK PRIORITIZATION

Snow finds the software vulnerabilities in your organization by cross-referencing normalized data against NIST's National Vulnerability Database* and ranks them in order of criticality. Snow further references data against our own unique database of applications that may contain personal data risk.

In addition, Snow flags software and hardware that has exceeded its End-of-Life or End-of-Support date, allowing visibility of business-critical functions compromised when running on out-of-date systems.

To support regulatory compliance, applications are classified based on whether they may process personal data (and what type).

AUTOMATED AND INTERACTIVE

Say goodbye to Excel. Snow Risk Monitor surveys the IT environment, finding vulnerabilities automatically so you don't have to.

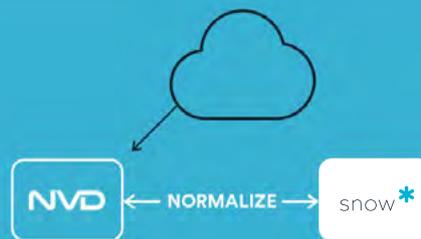
Explore your risk landscape in intuitive dashboards, allowing you to dynamically pinpoint the exact application, version and device with a vulnerability or personal data risk. Manage and reduce the risks associated with applications, whilst supporting the security that underpins regulations.

Step One



Our scanning capabilities identify all devices, users and applications across on-premises, cloud and mobile.

Step Two



Application data is recognized, and Snow's powerful technology is used to cross-reference normalized data with the NVD for vulnerabilities or with Snow's own unique information of applications containing a personal data risk.

Step Three



Report highlights risks on devices, along with information such as severity scoring or personal data categorization.

ABOUT SNOW SOFTWARE

Snow Software is changing the way organizations understand and manage their technology consumption. Our technology intelligence platform provides comprehensive visibility and contextual insight across software, SaaS, hardware and cloud. With Snow, IT leaders can effectively optimize resources, enhance performance and enable operational agility in a hybrid world. To learn more, visit www.snowsoftware.com.

